UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 10/538,289 | 06/10/2005 | Michiaki Tatsubori | JP920020206US1 | 9237 |

47069 7590 11/17/2008
KONRAD RAYNES & VICTOR, LLP
ATTN: IBM54
315 SOUTH BEVERLY DRIVE, SUITE 210
BEVERLY HILLS, CA 90212

| EXAMINER | |
|---|---|
| TURNER, ASHLEY D | |

| ART UNIT | PAPER NUMBER |
|---|---|
| 2454 | |

| NOTIFICATION DATE | DELIVERY MODE |
|---|---|
| 11/17/2008 | ELECTRONIC |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

krvuspto@ipmatters.com

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 10/538,289 | TATSUBORI ET AL. | |
| | Examiner | Art Unit | |
| | ASHLEY D. TURNER | 2454 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *28 August 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *31-34 and 40-46* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *31-34 and 40-46* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

## DETAILED ACTION

### *Claim Rejections - 35 USC § 103*

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claim 31-39 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Schneider (U.S. 6,785,728 B1), in view of Bailey (U.S. 5,349,663).

Referring to claim 31

Referring to claim 31 Schneider discloses a method, comprising: receiving a call request from a user with to execute an object; determining an access authority for the user (Col.9 lines 40-65 and Col. 10 lines 1-30 FIG. 3 is a conceptual overview of access control database 301. The primary function of the database is to respond to an access request 309 from access filter 203 which identifies a user and an information resource with an indication 311 of whether the request will be granted or denied. The request will be granted if both of the following are true: The user belongs to a user group which

data base 301 indicates may access an information set to which the information resource belongs; and the request has a trust level which is at least as high as a sensitivity level belonging to the information resource. Each user belongs to one or more of the user groups and each information resource belongs to one or more information sets; if none of the user groups that the user belongs to is denied access to an information set that the resource belongs to and any of the user groups that the user belongs to is allowed access to any of the information sets that the information resource belongs to, the user may access the information resource, provided that the request has the requisite trust level. The sensitivity level of a resource is simply a value that indicates the trust level required to access the resource. In general, the greater the need to protect the information resource, the higher its sensitivity level. The trust level of a request has a number of components: the trust level of the identification technique used to identify the user; for example, identification of a user by a token has a higher trust level than identification of the user by IP address. The trust level of the path taken by the access request through the network; for example, a path that includes the Internet has a lower trust level than one that includes only internal networks. If the access request is encrypted, the trust level of the encryption technique used; the stronger the encryption technique, the higher the trust level. The trust level of the identification technique and the trust level of the path are each considered separately. The trust level of the path may, however, be affected by the trust level of the encryption technique used to encrypt the access request. If the request is encrypted with an encryption technique whose trust level is higher that the trust level of a portion of the

path, the trust level of the portion is increased to the trust level of the encryption technique. Thus, if the trust level of a portion of a path is less than required for the sensitivity level of the resource, the problem can be solved by encrypting the access request with an encryption technique that has the necessary trust level. The information contained in database 301 may be divided into five broad categories: user identification information 313, which identifies the user; user groups 315, which defines the groups the users belong to; information resources 320, which defines the individual information items subject to protection and specifies where to find them; information sets 321, which defines groups of information resources); and searching a storage section storing execution results for a previous execution of the object prior to executing the call request and in response to determining that the user access authority permits access to the methods called by the object. (Col. 26 lines 27-40 The IntraMap interface lets the user sort Resource List 1803 by information sets, locations, or services. To do this, the user selects the way he or she wishes to sort the resource list in sort field 1809. The user may also specify the order in which the categories are used in the sort. The interface further has a search function. To do a search, the user enters a search string in FIND field 1807. The resource list and the resource descriptions for the resources on it are then searched in the order specified in sort field 1809. The search simply looks for whole or partial word matches. It is not case sensitive. The first match is displayed, and function keys may be used to navigate to other matches. Of course, if a user has not checked a service type in service type field 1811, resources of that service type are not involved in either sorting or searching). Schneider did not disclose acquiring an object

access authority set for the object indicating access authorities for methods called by the object; comparing the user access authority and the object access authority set to determine whether the user access authority permits access to the methods called by the object. The general concept of acquiring an object access authority set for the object indicating access authorities for methods called by the object; comparing the user access authority and the object access authority set to determine whether the user access authority permits access to the methods called by the object is well known in the art as taught by Bailey. Bailey discloses acquiring an object access authority set for the object indicating access authorities for methods called by the object; comparing the user access authority and the object access authority set to determine whether the user access authority permits access to the methods called by the object. (Col. 9 lines 60-68 and Col.10 lines 1-2 It is now possible to determine if a user has either system or group authority to access an OBJECT by comparing DOMKEYs. When the Users attempts to access the OBJECT, each of the Users ADKs would be compared to the ODK of the OBJECT. If any of the comparisons match for the full length of the Users ADK over the Object's ODK, the Users has access to or authority over the OBJECT. If all of the comparisons fail, then the User is not authorized via system or group attributes to access the OBJECT, nor does the user have authority over the OBJECT). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Schneider to includeacquiring an object access authority set for the object indicating access authorities for methods called by the object; comparing the user access authority and the object access authority set to determine whether the user access

authority permits access to the methods called by the object in order to provide its Hosts with the added value and incremental revenues of traditional affiliate programs, but the company also enables Hosts to control the customer experience before, during, and after the purchase transaction.

Referring to claim 32

Referring to claim 32 Schneider and Bailey disclose all the limitations of claim 32 which is described above. Schneider also discloses wherein the call request is received over a network, and wherein the execution results are transmitted over the network and wherein the call request with respect to the object comprises a request for Web services. (Col. 2 lines 6-24 FIG. 1 shows techniques presently used to increase security in networks that are accessible via the Internet. FIG. 1 shows network 101, which is made up of two separate internal networks 103(A) and 103(B) that are connected by Internet 111. Networks 103(A) and 103(B) are not generally accessible, but are part of the Internet in the sense that computer systems in these networks have Internet addresses and employ Internet protocols to exchange information. Two such computer systems appear in FIG. 1 as requestor 105 in network 103(A) and server 113 in network 103(b). Requestor 105 is requesting access to data which can be provided by server 113. Attached to server 113 is a mass storage device 115 that contains data 117 which is being requested by requester 105. Of course, for other data, server 113

may be the requester and requestor 105 the server. Moreover, access is to be understood in the present context as any operation which can read or change data stored on server 113 or which can change the state of server 113. In making the request, requestor 105 is using one of the standard TCP/IP protocols. As used here, a protocol is a description of a set of messages that can be used to exchange information between computer systems. The actual messages that are sent between computer systems that are communicating according to a protocol are collectively termed a session. During the session, Requestor 105 sends messages according to the protocol to server 113's Internet address and server 113 sends messages according to the protocol to requester 105's Internet address. Both the request and response will travel between internal network 103(A) and 103(B) by Internet 111. If server 113 permits requestor 105 to access the data, some of the messages flowing from server 113 to requestor 105 in the session will include the requested data 117. The software components of server 113 which respond to the messages as required by the protocol are termed a service.)

Referring to claim 34

Referring to claim 34 Schneider and Bailey disclose all the limitations of claim 34 which is described above. Schneider also discloses passing the call request to an object executor in response to determining that the storage section does not store execution results for the previous execution of the object subject to the call request. (Col.9 lines

40-65 and Col. 10 lines 1-30 FIG. 3 is a conceptual overview of access control database 301. The primary function of the database is to respond to an access request 309 from access filter 203 which identifies a user and an information resource with an indication 311 of whether the request will be granted or denied. The request will be granted if both of the following are true: The user belongs to a user group which data base 301 indicates may access an information set to which the information resource belongs; and the request has a trust level which is at least as high as a sensitivity level belonging to the information resource. Each user belongs to one or more of the user groups and each information resource belongs to one or more information sets; if none of the user groups that the user belongs to is denied access to an information set that the resource belongs to and any of the user groups that the user belongs to is allowed access to any of the information sets that the information resource belongs to, the user may access the information resource, provided that the request has the requisite trust level. The sensitivity level of a resource is simply a value that indicates the trust level required to access the resource. In general, the greater the need to protect the information resource, the higher its sensitivity level. The trust level of a request has a number of components: the trust level of the identification technique used to identify the user; for example, identification of a user by a token has a higher trust level than identification of the user by IP address. The trust level of the path taken by the access request through the network; for example, a path that includes the Internet has a lower trust level than one that includes only internal networks. If the access request is encrypted, the trust level of the encryption technique used; the stronger the encryption technique, the higher

the trust level. The trust level of the identification technique and the trust level of the path are each considered separately. The trust level of the path may, however, be affected by the trust level of the encryption technique used to encrypt the access request. If the request is encrypted with an encryption technique whose trust level is higher that the trust level of a portion of the path, the trust level of the portion is increased to the trust level of the encryption technique. Thus, if the trust level of a portion of a path is less than required for the sensitivity level of the resource, the problem can be solved by encrypting the access request with an encryption technique that has the necessary trust level. The information contained in database 301 may be divided into five broad categories: user identification information 313, which identifies the user; user groups 315, which defines the groups the users belong to; information resources 320, which defines the individual information items subject to protection and specifies where to find them; information sets 321, which defines groups of information resources)

Referring to claim 40

Referring to claim 40 Schneider and Bailey discloses all the limitations of claim 40 which is described above. Bailey also discloses determining methods called by the object; determining an access authority for each determined method; generating the object access authority set to comprise the determined access authorities of the determined methods, wherein the object access authority set indicates access

authorities needed to execute the determined methods. (Col. 9 lines 60-68 and Col.10 lines 1-2 It is now possible to determine if a user has either system or group authority to access an OBJECT by comparing DOMKEYs. When the Users attempts to access the OBJECT, each of the Users ADKs would be compared to the ODK of the OBJECT. If any of the comparisons match for the full length of the Users ADK over the Object's ODK, the Users has access to or authority over the OBJECT. If all of the comparisons fail, then the User is not authorized via system or group attributes to access the OBJECT, nor does the user have authority over the OBJECT).

Referring to claim 41

Referring to claim 41 Schneider and Bailey discloses all the limitations of claim 41 which is described above. Scheneider also discloses wherein determining the access authority for each determined method calling additional methods comprises: determining the access authorities of the additional methods called by the method, wherein the object access authority set for the method additionally includes the determined access authorities of the additional methods called by the method. (Col.9 lines 40-65 and Col. 10 lines 1-30 FIG. 3 is a conceptual overview of access control database 301. The primary function of the database is to respond to an access request 309 from access filter 203 which identifies a user and an information resource with an indication 311 of whether the request will be granted or denied. The request will be granted if both of the following are true: The user belongs to a user group which data

base 301 indicates may access an information set to which the information resource belongs; and the request has a trust level which is at least as high as a sensitivity level belonging to the information resource. Each user belongs to one or more of the user groups and each information resource belongs to one or more information sets; if none of the user groups that the user belongs to is denied access to an information set that the resource belongs to and any of the user groups that the user belongs to is allowed access to any of the information sets that the information resource belongs to, the user may access the information resource, provided that the request has the requisite trust level. The sensitivity level of a resource is simply a value that indicates the trust level required to access the resource. In general, the greater the need to protect the information resource, the higher its sensitivity level. The trust level of a request has a number of components: the trust level of the identification technique used to identify the user; for example, identification of a user by a token has a higher trust level than identification of the user by IP address. The trust level of the path taken by the access request through the network; for example, a path that includes the Internet has a lower trust level than one that includes only internal networks. If the access request is encrypted, the trust level of the encryption technique used; the stronger the encryption technique, the higher the trust level. The trust level of the identification technique and the trust level of the path are each considered separately. The trust level of the path may, however, be affected by the trust level of the encryption technique used to encrypt the access request. If the request is encrypted with an encryption technique whose trust level is higher that the trust level of a portion of the path, the trust level of the portion is

increased to the trust level of the encryption technique. Thus, if the trust level of a portion of a path is less than required for the sensitivity level of the resource, the problem can be solved by encrypting the access request with an encryption technique that has the necessary trust level. The information contained in database 301 may be divided into five broad categories: user identification information 313, which identifies the user; user groups 315, which defines the groups the users belong to; information resources 320, which defines the individual information items subject to protection and specifies where to find them; information sets 321, which defines groups of information resources)

Referring to claim 42

Referring to claim 42 Schneider and Bailey discloses all the limitations of claim 42 which is described above. Scheneider also discloses wherein access to the execution results is not granted to the user if the access authority for one determined method is unknown. (Col.9 lines 40-65 and Col. 10 lines 1-30 FIG. 3 is a conceptual overview of access control database 301. The primary function of the database is to respond to an access request 309 from access filter 203 which identifies a user and an information resource with an indication 311 of whether the request will be granted or denied. The request will be granted if both of the following are true: The user belongs to a user group which data base 301 indicates may access an information set to which the information resource belongs; and the request has a trust level which is at least as high as a sensitivity level belonging to the information resource. Each user belongs to one or

more of the user groups and each information resource belongs to one or more information sets; if none of the user groups that the user belongs to is denied access to an information set that the resource belongs to and any of the user groups that the user belongs to is allowed access to any of the information sets that the information resource belongs to, the user may access the information resource, provided that the request has the requisite trust level. The sensitivity level of a resource is simply a value that indicates the trust level required to access the resource. In general, the greater the need to protect the information resource, the higher its sensitivity level. The trust level of a request has a number of components: the trust level of the identification technique used to identify the user; for example, identification of a user by a token has a higher trust level than identification of the user by IP address. The trust level of the path taken by the access request through the network; for example, a path that includes the Internet has a lower trust level than one that includes only internal networks. If the access request is encrypted, the trust level of the encryption technique used; the stronger the encryption technique, the higher the trust level. The trust level of the identification technique and the trust level of the path are each considered separately. The trust level of the path may, however, be affected by the trust level of the encryption technique used to encrypt the access request. If the request is encrypted with an encryption technique whose trust level is higher that the trust level of a portion of the path, the trust level of the portion is increased to the trust level of the encryption technique. Thus, if the trust level of a portion of a path is less than required for the sensitivity level of the resource, the problem can be solved by encrypting the access

request with an encryption technique that has the necessary trust level. The information contained in database 301 may be divided into five broad categories: user identification information 313, which identifies the user; user groups 315, which defines the groups the users belong to; information resources 320, which defines the individual information items subject to protection and specifies where to find them; information sets 321, which defines groups of information resources).

Referring to claim 43

Referring to claim 43 Schneider and Bailey discloses all the limitations of claim 43 which is described above. Scheneider also discloses wherein the object is executed even if access to the execution results is not granted. (Col.9 lines 40-65 and Col. 10 lines 1-30 FIG. 3 is a conceptual overview of access control database 301. The primary function of the database is to respond to an access request 309 from access filter 203 which identifies a user and an information resource with an indication 311 of whether the request will be granted or denied. The request will be granted if both of the following are true: The user belongs to a user group which data base 301 indicates may access an information set to which the information resource belongs; and the request has a trust level which is at least as high as a sensitivity level belonging to the information resource. Each user belongs to one or more of the user groups and each information resource belongs to one or more information sets; if none of the user groups that the user belongs to is denied access to an information set that the resource belongs to and any of the user groups that the user belongs to is allowed access to any of the

information sets that the information resource belongs to, the user may access the information resource, provided that the request has the requisite trust level. The sensitivity level of a resource is simply a value that indicates the trust level required to access the resource. In general, the greater the need to protect the information resource, the higher its sensitivity level. The trust level of a request has a number of components: the trust level of the identification technique used to identify the user; for example, identification of a user by a token has a higher trust level than identification of the user by IP address. The trust level of the path taken by the access request through the network; for example, a path that includes the Internet has a lower trust level than one that includes only internal networks. If the access request is encrypted, the trust level of the encryption technique used; the stronger the encryption technique, the higher the trust level. The trust level of the identification technique and the trust level of the path are each considered separately. The trust level of the path may, however, be affected by the trust level of the encryption technique used to encrypt the access request. If the request is encrypted with an encryption technique whose trust level is higher that the trust level of a portion of the path, the trust level of the portion is increased to the trust level of the encryption technique. Thus, if the trust level of a portion of a path is less than required for the sensitivity level of the resource, the problem can be solved by encrypting the access request with an encryption technique that has the necessary trust level. The information contained in database 301 may be divided into five broad categories: user identification information 313, which identifies the user; user groups 315, which defines the groups the users belong to; information

resources 320, which defines the individual information items subject to protection and specifies where to find them; information sets 321, which defines groups of information resources).

Referring to claim 44

Referring to claim 44 Schneider and Bailey discloses all the limitations of claim 42 which is described above. Scheneider also discloses storing execution results from the object executor in response to executing the object of the call request with the access authority set for the object and an object name. (Col.9 lines 40-65 and Col. 10 lines 1-30 FIG. 3 is a conceptual overview of access control database 301. The primary function of the database is to respond to an access request 309 from access filter 203 which identifies a user and an information resource with an indication 311 of whether the request will be granted or denied. The request will be granted if both of the following are true: The user belongs to a user group which data base 301 indicates may access an information set to which the information resource belongs; and the request has a trust level which is at least as high as a sensitivity level belonging to the information resource. Each user belongs to one or more of the user groups and each information resource belongs to one or more information sets; if none of the user groups that the user belongs to is denied access to an information set that the resource belongs to and any of the user groups that the user belongs to is allowed access to any of the information sets that the information resource belongs to, the user may access the information resource, provided that the request has the requisite trust level. The

sensitivity level of a resource is simply a value that indicates the trust level required to access the resource. In general, the greater the need to protect the information resource, the higher its sensitivity level. The trust level of a request has a number of components: the trust level of the identification technique used to identify the user; for example, identification of a user by a token has a higher trust level than identification of the user by IP address. The trust level of the path taken by the access request through the network; for example, a path that includes the Internet has a lower trust level than one that includes only internal networks. If the access request is encrypted, the trust level of the encryption technique used; the stronger the encryption technique, the higher the trust level. The trust level of the identification technique and the trust level of the path are each considered separately. The trust level of the path may, however, be affected by the trust level of the encryption technique used to encrypt the access request. If the request is encrypted with an encryption technique whose trust level is higher that the trust level of a portion of the path, the trust level of the portion is increased to the trust level of the encryption technique. Thus, if the trust level of a portion of a path is less than required for the sensitivity level of the resource, the problem can be solved by encrypting the access request with an encryption technique that has the necessary trust level. The information contained in database 301 may be divided into five broad categories: user identification information 313, which identifies the user; user groups 315, which defines the groups the users belong to; information resources 320, which defines the individual information items subject to protection and

specifies where to find them; information sets 321, which defines groups of information resources).

Referring to claim 45

Referring to claim 45 Schneider and Bailey discloses all the limitations of claim 45 which is described above. Scheneider also discloses returning the execution results to the user having user access authority permitting access to the object. (Col.9 lines 40-65 and Col. 10 lines 1-30 FIG. 3 is a conceptual overview of access control database 301. The primary function of the database is to respond to an access request 309 from access filter 203 which identifies a user and an information resource with an indication 311 of whether the request will be granted or denied. The request will be granted if both of the following are true: The user belongs to a user group which data base 301 indicates may access an information set to which the information resource belongs; and the request has a trust level which is at least as high as a sensitivity level belonging to the information resource. Each user belongs to one or more of the user groups and each information resource belongs to one or more information sets; if none of the user groups that the user belongs to is denied access to an information set that the resource belongs to and any of the user groups that the user belongs to is allowed access to any of the information sets that the information resource belongs to, the user may access the information resource, provided that the request has the requisite trust level. The sensitivity level of a resource is simply a value that indicates the trust level required to

access the resource. In general, the greater the need to protect the information resource, the higher its sensitivity level. The trust level of a request has a number of components: the trust level of the identification technique used to identify the user; for example, identification of a user by a token has a higher trust level than identification of the user by IP address. The trust level of the path taken by the access request through the network; for example, a path that includes the Internet has a lower trust level than one that includes only internal networks. If the access request is encrypted, the trust level of the encryption technique used; the stronger the encryption technique, the higher the trust level. The trust level of the identification technique and the trust level of the path are each considered separately. The trust level of the path may, however, be affected by the trust level of the encryption technique used to encrypt the access request. If the request is encrypted with an encryption technique whose trust level is higher that the trust level of a portion of the path, the trust level of the portion is increased to the trust level of the encryption technique. Thus, if the trust level of a portion of a path is less than required for the sensitivity level of the resource, the problem can be solved by encrypting the access request with an encryption technique that has the necessary trust level. The information contained in database 301 may be divided into five broad categories: user identification information 313, which identifies the user; user groups 315, which defines the groups the users belong to; information resources 320, which defines the individual information items subject to protection and specifies where to find them; information sets 321, which defines groups of information resources).

Referring to claim 46

Referring to claim 46 Schneider and Bailey discloses all the limitations of claim 46 which is described above. Scheneider also discloses receiving a subsequent call request for the object from the user; returning the execution results to the user in response to determining that the execution results are associated with the user without comparing the user access control to the object access authority. (Col.9 lines 40-65 and Col. 10 lines 1-30 FIG. 3 is a conceptual overview of access control database 301. The primary function of the database is to respond to an access request 309 from access filter 203 which identifies a user and an information resource with an indication 311 of whether the request will be granted or denied. The request will be granted if both of the following are true: The user belongs to a user group which data base 301 indicates may access an information set to which the information resource belongs; and the request has a trust level which is at least as high as a sensitivity level belonging to the information resource. Each user belongs to one or more of the user groups and each information resource belongs to one or more information sets; if none of the user groups that the user belongs to is denied access to an information set that the resource belongs to and any of the user groups that the user belongs to is allowed access to any of the information sets that the information resource belongs to, the user may access the information resource, provided that the request has the requisite trust level. The

sensitivity level of a resource is simply a value that indicates the trust level required to access the resource. In general, the greater the need to protect the information resource, the higher its sensitivity level. The trust level of a request has a number of components: the trust level of the identification technique used to identify the user; for example, identification of a user by a token has a higher trust level than identification of the user by IP address. The trust level of the path taken by the access request through the network; for example, a path that includes the Internet has a lower trust level than one that includes only internal networks. If the access request is encrypted, the trust level of the encryption technique used; the stronger the encryption technique, the higher the trust level. The trust level of the identification technique and the trust level of the path are each considered separately. The trust level of the path may, however, be affected by the trust level of the encryption technique used to encrypt the access request. If the request is encrypted with an encryption technique whose trust level is higher that the trust level of a portion of the path, the trust level of the portion is increased to the trust level of the encryption technique. Thus, if the trust level of a portion of a path is less than required for the sensitivity level of the resource, the problem can be solved by encrypting the access request with an encryption technique that has the necessary trust level. The information contained in database 301 may be divided into five broad categories: user identification information 313, which identifies the user; user groups 315, which defines the groups the users belong to; information resources 320, which defines the individual information items subject to protection and

specifies where to find them; information sets 321, which defines groups of information resources).

Claim 33 are rejected under 35 U.S.C. 103 (a) as being unpatentable over Schneider (U.S. 6,785,728 B1), in view of Bailey (U.S. 5,349,663) further in view of Ross (US 6,629,135 B1).

Referring to claim 33

Referring to claim 33 Schneider and Bailey discloses all the limitations of claim 33 which is described above. Schneider did not discloses transmitting the execution results for the previous execution of the object prior to executing the call request with respect to the object in response to determining that the storage section stores the execution results for the previous execution of the object subject to the call request. The general concept of transmitting the execution results for the previous execution of the object prior to executing the call request with respect to the object in response to determining that the storage section stores the execution results for the previous execution of the object subject to the call request is well known in the art as taught by Ross. Ross discloses transmitting the execution results for the previous execution of the object prior to executing the call request with respect to the object in response to determining that the storage section stores the execution results for the previous execution of the object subject to the call request(Col 5 lines 56-61 Object Cache 250. The object cache

contains the responses to previously submitted requests. All items in the cache are marked with an expiration time that is set at the time they are originally retrieved. The purpose of this layer is to reduce the load on the application tier). It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Schneider in order to include transmitting the execution results for the previous execution of the object prior to executing the call request with respect to the object in response to determining that the storage section stores the execution results for the previous execution of the object subject to the call request in order to provide its Hosts with the added value and incremental revenues of traditional affiliate programs, but the company also enables Hosts to control the customer experience before, during, and after the purchase transaction.

***Conclusion***

Arguments are deemed moot in view of the new grounds of rejection necessitated by the amendment.

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the

shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ashley D. Turner whose telephone number is 571-270-1603. The examiner can normally be reached on Monday thru Friday 7:30a.m.-5:00p.m..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nathan J. Flynn can be reached on 571-272-1915. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Ashley D Turner
Examiner
Art Unit 2154

/Nathan J. Flynn/

Supervisory Patent Examiner, Art Unit 2454